AF

PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Applicants: Narayanaswami et al.

Examiner: Rashawn N. Tillery

Serial No.: 09/080,517

Group Art Unit: 2612

Filed: May 18, 1998

Docket: 8728-118 (YO998-095)

For: **An Image Capturing System And Method For Automatically Watermarking Recorded Parameters For Providing Digital Image Verification**

Request For Reinstatement of Appeal under 37 C.F.R. § 1.193(b)(2)

This is a request to reinstate the Appeal that was commenced in connection with the above-referenced application by Notice of Appeal filed on November 19, 2003 and Appeal Brief filed on March 17, 2004. In response to Applicants' Appeal Brief, a new Final Office Action was mailed on June 21, 2004 (Paper No. 23) to re-open prosecution and assert new grounds of rejection. Now, in support of Applicants' request to reinstate the Appeal, a Supplemental Appeal Brief is submitted herewith to address the new grounds for rejection.

CERTIFICATE OF MAILING 37 C.F.R. §1.8(a)

I hereby certify that this correspondence is being deposited with the United States Postal.Service as first class mail, postage paid in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA. 22313, Mail Stop- Appeal Brief Patents, on November 22, 2004.

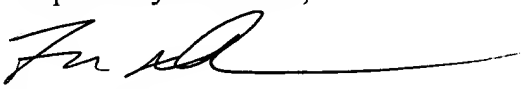
Dated: 11/22/04

Frank DeRosa

It is believed that there is no fee associated with this Request. If additional fees are required, please charge such fees to Deposit Account 50-0510/IBM. A duplicate copy of this paper is enclosed for accounting.

Dated: 11/22/04

Respectfully submitted,



Frank DeRosa
Reg. No. 43,584
Attorney for Applicant(s)

F. Chau & Associates, LLC
130 Woodbury Road
Woodbury, New York 11797
TEL.: (516) 692-8888
FAX: (516) 692-8889

PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Applicants: Narayanaswami et al.

Examiner: Rashawn N. Tillery

Serial No.: 09/080,517

Group Art Unit: 2612

Filed: May 18, 1998

Docket: 8728-118 (YO998-095)

For: **An Image Capturing System And Method For Automatically Watermarking Recorded Parameters For Providing Digital Image Verification**

SUPPLEMENTAL APPEAL BRIEF

Appeal from Group 2612

F. Chau & Associates, LLC
130 Woodbury Road
Woodbury, New York 11797
TEL: (516) 692-8888
FAX: (516) 692-8889
Attorneys for Appellants

TABLE OF CONTENTS **Page(s)**

I. INTRODUCTION

This Appeal was initially commenced by a Notice of Appeal (filed on November 19, 2003) and an Appeal Brief (filed on March 17, 2004), in response to a Final Office Action (Paper No. 18) (hereinafter, the "FINAL ACTION), finally rejecting claims 1-22 of the above-identified application.

In response to Applicants' Appeal Brief, a new Final Office Action was mailed on June 21, 2004 (Paper No. 23) (hereinafter, the "NEW ACTION") to re-open prosecution and assert new grounds of rejection. Applicants have submitted herewith a Request to Reinstate the Appeal under 37 C.F.R. 1.193(b)(2). In support of such Request, Applicants hereby respectfully submit this Supplemental Appeal Brief to address the newly asserted grounds for rejection.

II. REAL PARTY IN INTEREST

The real party in interest for the above-identified application is International Business Machines (IBM) Corporation, the assignee of the entire right, title and interest in and to the subject application by virtue of an assignment of record in the U.S. Patent and Trademark Office.

III. RELATED APPEALS AND INTERFERENCES

There are no Appeals or Interferences known to Applicant, Applicant's representatives or the Assignee, which would directly affect or be indirectly affected by or have a bearing on the Board's decision in the pending Appeal.

IV. STATUS OF CLAIMS

Claims 1-22 are pending. Claims 1 and 4-22 stand rejected and are under appeal. The NEW ACTION indicates (on page 9) that claims 2 and 3 comprise allowable subject matter. The currently pending claims, including those claims on appeal, are set forth in the attached Appendix. Claims 1, 13 and 18 are independent claims. Claims 2-12 depend directly or indirectly from claim 1. Claims 14-17 and 21 depend directly or indirectly from claim 13. Claims 19-20 and 22 depend directly or indirectly from claim 18.

V. STATUS OF AMENDMENTS

No after final Amendments were filed in this case subsequent to the NEW ACTION.

VI. SUMMARY OF THE INVENTION

In general, the claimed inventions are directed to systems and methods for verifying the authenticity of digital images using watermarking methods. For example, an image capturing system according to an embodiment of the invention employs methods for automatically recording one or more camera/image parameters associated with a captured image, and automatically watermarking the recorded camera/image parameter(s) within the captured image. The camera/image parameters that can be automatically recorded with a captured image include, for example, names of geographic locations, altitude, longitude, time, date, photographer identification, as well as image data such as light intensity, shutter speed and flash status, etc. The watermarking process is implemented to invisibly watermark (i.e., hide) one or more of the recorded parameters within the captured image. The original recorded parameters associated with the captured image are stored for subsequent access.

The authenticity of the digital image can subsequently be verified by extracting the watermarked parameters from the digital image, and comparing the extracted parameters with the original recorded parameters (associated with the digital image) to determine whether the recorded parameters match the extracted parameters. Since the recorded parameters are watermarked into the image, it is difficult to modify the image without affecting the watermarked data. Therefore, if the extracted data appears corrupted (the extracted parameters does not match the recorded parameters associated with the image), it is an indication that the image is not authentic and has been modified or otherwise tampered with.

Independent claims 1, 13 and 18 are representative of claimed inventions that embody features of the invention as generally described above, and such claims are reproduced hereafter for ease of reference:

1. *An image capturing system for automatically recording and watermarking a plurality of parameters in a captured image, comprising:*

a central processing unit for controlling a plurality of functions and operations of said system;

image capture means, operatively connected to said central processing unit, for generating a digital image of an observed image frame and for generating a plurality of image data associated with said generation of said image;

wireless communication means, operatively connected to said central processing unit, for receiving object data from objects in said observed image frame when said image is generated, said object data comprising object identification information;

geographic location determining means, operatively connected to said central processing unit, for determining geographic coordinates of said system when said digital image is generated;

means for determining a time and a date when said image is generated;

information receiving means, operatively coupled to said central processing unit, for

receiving user data associated with a user of said system when said digital image is generated, said user data comprising user identification information;

image processing means for receiving said plurality of parameters and recording said plurality of parameters with said generated digital image, said plurality of parameters including said plurality of image data, said object data, said time data, said date data, said location data, and said user data; and

means, operatively coupled to said image processing means, for watermarking said plurality of parameters into said image.

13. *In an image capturing system, a method for authenticating a captured image, comprising the steps of:*

measuring a plurality of parameters associated with said captured image;

watermarking said plurality of parameters into said captured image to generate a watermarked image, and generating a verification key associated with said watermarked parameters;

extracting said plurality of parameters from said watermarked image with said associated verification key; and

comparing said extracted plurality of parameters from said watermarked image with said measured plurality of parameters associated with said captured image, whereby said captured image is authenticated if said extracted parameters match with said measured parameters.

18. *A method for verifying the authenticity of a captured image, said captured image being generated by an image capturing system having means for measuring a plurality of parameters associated with said captured image and means for watermarking said plurality of parameters within said captured image, said method comprising the steps of:*

specifying at least one of said plurality of parameters to be measured and watermarked by said image capturing system;

capturing an image of a desired object with said image capturing system;

watermarking said captured image of said object with said specified parameters;

generating a corresponding verification key based on said watermarked parameters;

storing said watermarked image and said corresponding verification key;

retrieving said watermarked image and said corresponding verification key;

extracting from said watermarked image said watermarked parameters using said verification key;

comparing said extracted parameters with said specified parameters to determine if said extracted parameters match said specified parameters.

VII. ISSUES

(1) Claims 1, 4-8 and 12-22 stand rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 5,499,294 to Friedman in view of U.S. Patent No. 6,192,138 to Yamadaji.

Thus, one issue on appeal is whether the combination of Yamadaji and Friedman is legally sufficient to establish a *prima facie* case of obviousness against claims 1, 4-8 and 12-22.

(2) Claim 9 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Friedman in view of Yamadaji in further view of U.S. Patent No. 5,799,082 to Murphy et al.

Thus, another issue on appeal is whether the combination of Yamadaji, Friedman and Murphy is legally sufficient to establish a *prima facie* case of obviousness against claim 9.

(3) Claims 10-11 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Friedman in view of Yamadaji in further view of U.S. Patent No. 5,335,072 to Tanaka et al.

Thus, another issue on appeal is whether the combination of Yamadaji, Friedman and Tanaka is legally sufficient to establish a *prima facie* case of obviousness against claims 10 and 11.

VIII. GROUPING OF CLAIMS

For purposes of this appeal:

For Issue (1) above:

(i) Claims 1, 4, 5 and 6 stand or fall independently, and claims 7, 8 and 12 stand or fall with their respective base claims;

(ii) Claims 13, 14 and 21 stand or fall independently and claims 15, 16 and 17 stand or fall with their respective base claims; and

(iii) Claims 18, 19 and 22 stand or fall independently and claim 20 stands or falls with base claim 19.

For Issue (2) above:

Claim 9 stands or falls with Claim 1.

For Issue (3) above:

Claims 10 and 11 stand or fall with Claim 1.

IX. ARGUMENTS

A. The Combination of Friedman and Yamadaji is *Legally Deficient* to Support a *Prima Facie* Case Of Obviousness Against Claims 1, 13 or 18

In rejecting claims under 35 U.S.C. 103, the Examiner bears the initial burden of presenting a prima facie case of obviousness. In re Rijckaert, 9 F.3d 1531, 1532 (Fed. Cir. 1993). The burden of presenting a prima facie case of obviousness is only satisfied by showing some objective teaching in the prior art or that knowledge generally available to one of ordinary skill in the art would lead that individual to combine the relevant teachings of the references. In re Fine, 837 F.2d 1071, 1074 (Fed. Cir. 1988). A prima facie case of obviousness is established when

the teachings of the prior art itself would appear to have suggested the claimed subject matter to one of ordinary skill in the art. In re Bell, 991 F.2d 781, 782 (Fed. Cir. 1993). The suggestion to combine the references should come from the prior art, and the Examiner cannot use hindsight gleaned from the invention itself to pick and choose among related disclosures in the prior art to arrive at the claimed invention. In re Fine, 837 F.2d at 1075. If the Examiner fails to establish a prima facie case, the rejection is improper and must be overturned. In re Rijckaert, 9 F.3d at 1532 (citing In re Fine, 837 F.2d at 1074).

In the case at bar, Appellants respectfully submit that at the very minimum, the NEW ACTION fails to present any legally sufficient basis for establishing a *prima facie* case of obviousness of claims 1, 13 or 18 based on the combination of Friedman and Yamadaji. Indeed, as demonstrate below, other than conclusory assertions of obviousness based on hindsight reasoning, the Examiner has offered no reasonable explanation as to why one of ordinary skill in the art would have been motivated to combine the teachings of Friedman and Yamadaji to derive the inventions of claims 1, 13 or 18. Moreover, even assuming, *arguendo*, that Friedman of Yamadaji are legally combinable, the Examiner has failed to demonstrate how such combination discloses or suggests every element of the inventions of claims 1, 13 or 18.

The obviousness rejections of Claims 1, 13 and 18 as set forth in the NEW ACTION are based primarily on the teachings of Friedman as modified by the teachings of Yamadaji. The following discussion will begin with a brief description of Friedman and Yamadaji, followed by an explanation as to the *impropriety* of the obviousness rejections based on the combination of Friedman and Yamadaji.

Friedman* - *Image Authentication based on Digital Signature Protocol

In general, Friedman is directed to a digital camera having a processing architecture that enables authentication of a digital image using a "digital signature" scheme based on "public key encryption", which is well known in the art. In particular, Friedman discloses a camera having a processor that is equipped (by the manufacture) with an embedded "private key" that is unique to the camera. The camera processor includes means for computing an "*image hash*" of an image file (using a predetermined hash function) and means for encrypting the "*image hash*" using the "private key" to thereby generate a "digital signature" (i.e., the digital signature is the encrypted image hash). The image file and corresponding digital signature are separate entities that are stored in association together, and the digital signature is subsequently used for authenticating the corresponding image file as being free of alteration or modification. In particular, with the Friedman system, authentication of the image file includes: (i) accessing the stored image file and corresponding digital signature, (ii) computing an "image hash" of the accessed image file using the same predetermined hash function that was used to generate the original image hash; (iii) decrypting the corresponding digital signature using a "public key" to recover the original image hash (i.e., the secure image hash); and (iv) comparing the original (secure) image hash with the currently computed image hash of the accessed image file. If the original (secure) image hash matches the currently computed image hash, the accessed image file is deemed authentic (see generally, e.g., Friedman Abstract; Col. 4, lines 19-54; Col. 5, line 49, through Col. 6, line 52; FIGs. 3A~3C; and Claim 1 (Col. 11 21-37)).

Friedman further discloses certain information (e.g., date, time, etc.) may be added in a border region of an image file, which surrounds the digital image, and that the added information in the border region is included in the image file which is hashed and encrypted to generate a

digital signature (see generally, e.g., Friedman FIG. 4; and Col. 4, lines 55-66). Although Friedman discloses that such parameters in the image border are part of the image file that is hashed and encrypted to generate a digital signature, these border parameters are not necessary for the authentication because the digital signature can be generated by encrypting the image hash of an image file that contains no recorded parameters in its border. In other words, as explained above, the authentication is not based on the content of the image file, per se, but only on matching the secure image hash (obtained from decrypting the digital signature) and the computed image hash (obtained by hashing the image file in question) (see, e.g., Friedman Col. 5, line 49, through Col. 6, line 52).

Yamadaji - Copyright Protection Protocol using Watermarking

Yamadaji discloses a method for watermarking copyright information (images or textual) in an image for purposes of copyright protection of the image. The copyright data is stored in memory as a digital watermark and the digital watermark can be accessed and embedded within a captured image (see, e.g., Col. 8, line 12 – Col. 9, line 22).

(i) There is *No* Legally Sufficient Basis for Combining the Teachings of Friedman and Yamadaji to Support the Obviousness Rejections

The obviousness rejections of Claims 1, 13 and 18 as set forth in the NEW ACTION are based primarily on the teachings of Friedman as modified by the teachings of Yamadaji. Essentially, the Examiner contends that one of ordinary skill in the art would be motivated to combine the teachings of Yamadaji with Friedman to provide image authentication by *watermarking a plurality of parameters into a captured image,* as essentially claimed in claims 1, 13 and 18. As explained below, however, the Examiner's conclusions of obviousness and

basis for motivation are premised on nothing more than impermissible hindsight reasoning based on the teachings of the current specification. The Examiner's basis for rejecting claims 1, 13 and 18 is the same (see obviousness analysis set forth on pages 3-5 of the NEW ACTION), and thus the rejections of such claims will be discussed together.

In particular, the Examiner acknowledges that Friedman's method of digital image authentication is based on a public/private key and digital signature framework, and that recorded "parameter data" can be recorded in the border of an image. The Examiner further acknowledges that the "parameter data" in the border of the image can be hashed and encrypted together with the image to generate a digital signature. The Examiner further acknowledges that Friedman does not expressly disclose means for watermarking the parameters into the image (see page 5 of the NEW ACTION).

In an effort to cure the deficiencies of Friedman in this regard, the Examiner cites Yamadaji's disclosure of a method of embedding watermark data into an image, wherein the watermark data comprises a logo mark or trademark (see page 5 of the NEW ACTION). Then in a conclusory fashion, the Examiner contends (on page 5 of the NEW ACTION) that:

> *"It would have been obvious to one of ordinary skill in the art at the time of the invention was made to watermark Friedman's parameters into the image as well as record them. One would have been motivated to do so in an effort to safeguard the images against malicious manipulations while also protecting the proprietary rights by maintaining the integrity of the image content.*

It is respectfully submitted, however, that Examiner's grounds for obviousness based on Friedman and Yamadaji falls *woefully* short of that which is required to met the burden of

establishing a *prima facie* case of obviousness. Indeed, it is readily apparent that in an effort to establish obviousness, the Examiner used *hindsight reasoning* to selectively combine the "watermarking" teachings of Yamadaji with the "recorded parameters" teachings of Friedman to derive inventions of claims 1, 13 and 18. But the Examiner has offered no legally sufficient explanation as to how one of ordinary skill in the art would be motivated to combine the relevant teachings of the Friedman and Yamadaji to derive the claimed inventions, e.g., providing *digital image authentication by watermarking recorded parameters into an image.*

To begin, it is respectfully submitted that in the first instance, the Examiner's reliance on Yamadaji to cure the deficiencies of Friedman is misplaced. Indeed, although Yamadaji discloses "watermarking" in general, the express motivation behind Yamadaji's watermarking is to provide copyright protection (see, e.g., Yamadaji Abstract) There is nothing in Yamadaji that teaches using watermarking for protecting against image alteration for purposes of image authentication. In particular, as noted above, Yamadaji discloses the use of watermarking technology to embed copyright or trademark data into an JPEG or MPEG image data, which enables a copyright owner to confirm if a given digital image has been "copied" by unbedding the digital watermark from the copy of the image data according to a prescribed procedure (see, Col. 2, lines 43-58). In other words, Yamadaji teaches the use of watermarking for the purpose of identifying an illegal copy of the digital image data by restoring the copyright or other identification information.

In fact, in the Examiner's conclusion of obviousness as outlined above, the Examiner even acknowledges the teachings of Yamadaji in this regard, wherein Examiner cites the "*motivation*" for using Yamadaji's watermarking in the Friedman system as "... *also protecting the proprietary rights* ..." However, this misses the point because the claimed inventions make

use of watermarking of recorded parameters to invisibly embed such parameters into an image for purposes of digital image authentication and preventing alteration of such digital images, not protecting proprietary copyrights.

Thus, on a fundamental level, the Examiner failed to demonstrate how Yamadaji's teachings of *watermarking for copyright protection* would suggest to one of ordinary skill in the art the use of *watermarking for image authentication.* In any event, as explained hereafter, it is clear that the Examiner has failed to demonstrate how one of ordinary skill in the art would be motivated to combine Yamadaji's teachings of *watermarking for copyright protection* with Friedman's "recorded parameters" for purposes of image authentication.

To begin, although Friedman discloses "recorded parameters", i.e., information (e.g., time or date) that can be captured in the border region of a photograph (see, e.g., Fig. 4 of Friedman), Friedman does not disclose or even suggest the use of such "recorded parameters" specifically for purposes of image authentication. In particular, as explained above, Friedman provides image authentication using the well-known digital signature method by calculating a hash of an image file and comparing the calculated hash with a secure image hash obtained by decrypting a corresponding digital signature. If the computed hash and secure hash are the same, then the image is deemed authentic. As explained above, Friedman does not use recorded parameters, *per se*, for purposes of authentication, because the Friedman system can compute a hash of the image file and encrypt the image hash to generate the digital signature regardless of whether or not the image file has captured information in an image border region. In other words, to reiterate, although Friedman discloses a method for verifying the authenticity of an image and that certain parameters associated with a captured image may be recorded in an image border, the Friedman protocol does ***not*** rely on such recorded parameters for authentication, i.e., Friedman

does not explicitly use the recorded parameters to authenticate the image *vis-à-vis* the digital signature method.

In contrast to Friedman, as explained above, the claimed inventions provide authentication by watermarking (hiding) captured image parameters into the image itself. With the claimed inventions, it is the watermarked parameters that are actually used for authentication and the captured image itself contains the information (watermarked parameters) for authenticating the image. Again, the Friedman authentication protocol (based on digital signature technology) can be used for authentication regardless of whether or not recorded parameters are contained in the border of the image file.

Therefore, in view of Friedman's distinct teachings of a *digital signature method for image authentication which is independent of "recorded parameters"* and in view of Yamadaji's distinct teaching of *watermarking copyright information (images or textual) in an image for purposes of copyright protection of the image,* it is clear that other than through impermissible hindsight reasoning from Applicants' specification, the Examiner has failed to show that one of ordinary skill in the art would not be motivated to combine copyright watermarking as taught by Yamadaji with the digital signature system of Friedman to derive an authentication protocol based on watermarking of recorded parameters as essentially claimed. In other words, the Examiner has simply combined the "watermarking" of Yamadaji with the recorded parameters of Friedman without offering any legally sufficient basis or motivation to justify such combination. Indeed, on a fundamental neither Yamadaji nor Friedman disclose using embedded data in an image for authenticating the integrity of the image content.

(ii) The Combination of Friedman and Yamadaji Does Not Disclose or Fairly Suggest Various Elements of Claims 1, 13 or 18

Even assuming, *arguendo*, that the combination of Friedman and Yamadaji is deemed to be legally proper, it is respectfully submitted that the combination of Friedman and Yamadaji is *legally deficient* to support a *prima facie* case of obviousness against claims 1, 13 or 18 because at the very minimum, such combination does not disclose or fairly suggest, as a whole, the inventions of claims 1, 13 or 18, and in particular, such combination fails to disclose or suggest various elements of claims 1, 13 and 18.

To begin, Applicants reiterate that for at least the reasons given above, the combination of Friedman and Yamadaji does not disclose or suggest, in general, systems or methods for providing digital image authentication by the use of *watermarking a plurality of parameters into a captured image,* as essentially claimed in claims 1, 13 and 18.

Furthermore, with regard to Claim 1, it is respectfully submitted that the combination of Friedman and Yamadaji does not disclose or suggest a system for capturing images, wherein the system comprises *wireless communication means for receiving object data from objects in an observed image frame when the image is generated, wherein the object data comprises object identification information*. Nor does such combination disclose or suggest *information receiving means for receiving user data associated with a user of the system when the digital image is generated, wherein the user data comprises user identification information*. By way of example, FIG. 1 of Applicants' specification depicts an image capturing system (100) having a smart card reader (110), a Pan (Personal Area Network) receiver (122), an IR processor (118) or an RF processor (112), which can be used to obtain and record *user data comprising user identification information* such as the identity of the photographer (see, e.g., page 9, lines 3-22, of Applicants'

specification). The IR processor (118) or RF processor (112) can be used for communicating with objects being photographed so as to obtain and record *object data comprising object identification information* such as the name and identity of the object being photographed (see, e.g., page 9, line 23, through page 10, line 6, of Applicants' specification). These parameters, e.g., *object identification data* and *user identification data* can be recorded with the digital mage and watermarked into the image.

In the NEW ACTION, Examiner relies on Friedman as disclosing the above features of claim 1. However, it is respectfully submitted that Examiner's reliance on Friedman in this regard is erroneous and glaringly misplaced because Friedman clearly does not disclose recorded parameters including (a) object identification information and (b) user identification information, as essentially claimed in Claim 1.

In particular, with regard to element (a) above, Examiner relies on Friedman's disclosure of a range finder (13) (such as an acoustic, optical, laser or infrared) to capture range information of prominent objects in a scene (see, Friedman Col. 9, lines 42-46), essentially contending that the range information captured by the range finder (13) can be interpreted as *object data that comprises object identification information* (see, e.g., Pages 3-4 of the NEW ACTION). Although Friedman discloses a rangefinder to collect "range information" to determine the distance an object is from the camera, the Examiner's strained interpretation of "range data" as being "object identification data" as contemplated by the claimed invention is an exercise of intellectual dishonestly, as there is simply no reasonable basis for construing such "range information" as being "object identification" as claimed in claim 1. Indeed, it is readily apparent that the "distance" an object is to a camera is very different from the "identity" of the object being imaged.

Furthermore, with regard to element (b) above, Examiner relies on Friedman's disclosure (Col. 3, lines 1-11) of a "serial number" of a camera as being *user data that comprises user identification information* (see, e.g., Page 4 of the NEW ACTION). Friedman discloses that *each digital camera possess its own unique private/public key pair, wherein the public key can be placed on the camera's name plate as a "serial number" or recorded in the border region of an image file* (see, e.g., Friedman Col. 7, lines 58-64). However, it is unreasonable to construe a camera "serial number" as being *"user identification information" that is associated with the user of the imaging system when the digital image is captured by the user,* as essentially claimed in Claim 1. Indeed, in the Friedman system, the serial number (or public key) is associated with the camera itself, and not with the user of the camera *per se.* In fact, many different users can use the same camera and in such instance, the "serial number" or public key would clearly not provide information regarding the identity of the person using the camera.

Moreover, with respect to Claims 13 and 18, the combination of Friedman and Yamadaji does not disclose or suggest an authentication protocol that includes *extracting parameters from a watermarked image using an associated verification key, comparing the extracted parameters with the original recorded/measured parameters associated with the captured image to determine if the extracted parameters match the originally recorded/measured parameters*, as essentially claimed in claims 13 and 18.

In fact, it should be noted that in the NEW ACTION, the Examiner provides no explanation or specific grounds to support of the rejection of Claims 13 and 18, other than reliance on same grounds of rejection of claim 1 (see, pages 3-5 of the NEW ACTION). In relying on the grounds for the rejection of claim 1, however, the Examiner has failed to address various elements of claims 13 and 18. For example, Examiner has not explained how the

combination of Friedman and Yamadaji teaches or suggest authentication by, e.g., *comparing watermarked parameters, which are extracted from a captured image, with the original parameters associated with the captured image, to determine if the extracted parameters match the original parameters*, as essentially claimed in claims 13 and 18. In any event, as explained above, the combination of Friedman and Yamadaji does not teach watermarking parameters into an image for purposes of image authentication and, thus, it necessarily and logically follows that such combination does not teach or suggest "*extracting watermarked parameters from the watermarked image and comparing the extracted parameters with the original parameters*" to authenticate the image.

Thus, for at least the above reasons, claims 1, 13 and 18 are believed to be patentable and non-obvious over the combination of Friedman and Yamadaji.

B. The Combination of Friedman and Yamadaji Does Not Disclose or Suggest Elements of Claims 4-6, 14, 19, and 21-22

At the very least, dependent claims 4-6, 14, 19, and 21-22 are patentable and non-obvious over the combination of Friedman and Yamadaji in their own right. For instance, with respect to claim 6, Examiner admits that neither Friedman nor Yamadaji expressly disclose the claimed invention, but Examiner contends, in conclusory manner, that claim 6 would have been obvious to one of ordinary to *prevent the watermarking of an image if the quality of the image is altered above a threshold* (as recited in claim 6) since "it would be a waste of time and money to watermark a damage/unclear image" (see, Pages 5-6 of the NEW ACTION). In the first instance, Examiner's basis for obviousness misses the point, because the claimed invention contemplates preventing watermarking if the watermarking of the parameter into the image would affect the image quality, but not preventing watermarking of a damaged image as

interpreted by Examiner. In any event, assuming Examiner's interpretation of claim 6 to be proper, it is respectfully submitted that Examiner's grounds for obviousness in this regard is premised on some bald, unsupported assertion based on Examiner's view of what would be obvious to one of ordinary skill in the art.

Moreover, with respect to claims 4-5, 14 and 19, at least the reasons set forth above for claims 13 and 18, Examiner has provided no explanation as to how the combination of Friedman and Yamadaji teaches comparing the extracted parameters with the original recorded/measured parameters associated with the captured image. In particular, for each of claims 4, 5, 14 and 19, the Examiner's grounds for rejection is simply "see claim 1 above" (see, pages 5, 6 and 7 of the NEW ACTION). However, it is readily apparent that the grounds for rejection claim 1 are silent with respect to the claimed features of claims 4, 5, 14 and 19. Thus, the rejection is invalid on its face.

Finally, with respect to claims 21 and 22, for at least the same reasons give above for claim 1, Examiner has misconstrued Friedman as disclosing watermarked parameters that include object identification or user identification information.

C. CONCLUSION

Accordingly, for at least the above reasons, it is respectfully requested that the Board reverse all claim rejections under 35 U.S.C. 103(a).

Respectfully submitted,

Frank DeRosa
Reg. No. 43,584

F. Chau & Associates, LLC
130 Woodbury Road
Woodbury, New York 11797
TEL: (516) 692-8888
FAX: (516) 692-8889

APPENDIX A

1. An image capturing system for automatically recording and watermarking a plurality of parameters in a captured image, comprising:

a central processing unit for controlling a plurality of functions and operations of said system;

image capture means, operatively connected to said central processing unit, for generating a digital image of an observed image frame and for generating a plurality of image data associated with said generation of said image;

wireless communication means, operatively connected to said central processing unit, for receiving object data from objects in said observed image frame when said image is generated, said object data comprising object identification information;

geographic location determining means, operatively connected to said central processing unit, for determining geographic coordinates of said system when said digital image is generated;

means for determining a time and a date when said image is generated;

information receiving means, operatively coupled to said central processing unit, for receiving user data associated with a user of said system when said digital image is generated, said user data comprising user identification information;

image processing means for receiving said plurality of parameters and recording said plurality of parameters with said generated digital image, said plurality of parameters including said plurality of image data, said object data, said time data, said date data, said location data, and said user data; and

means, operatively coupled to said image processing means, for watermarking said plurality of parameters into said image.

2. The system of claim 1, further comprising means for specifying which of the plurality of parameters should be recorded with said image and for specifying which of said plurality of parameters should be watermarked in said image.

3. The system of claim 2, further comprising means for determining which of the plurality of parameters are specified to be recorded with said image and for determining which of the plurality of parameters are specified to be watermarked in said image.

4. The system of claim 1, further comprising means for extracting said watermarked parameters from said watermarked image.

5. The system of claim 4, further comprising means for comparing said extracted parameters with corresponding recorded parameters of said image to authenticate said image.

6. The system of claim 1, further comprising means for preventing said watermarking of said images if an image quality of said image is altered above a threshold.

7. The system of claim 1, further comprising image compression means, operatively coupled to said image processing means, for compressing said image.

8. The system of claim 7, wherein said plurality of parameters are watermarked in one of said compressed image and said image.

9. The system of claim 1, further comprising orientation determining means, operatively coupled to said central processing unit, for determining orientation data of said system when said digital image is generated; said orientation data being one of said plurality of parameters.

10. The system of claim 1, further comprising

means for receiving one of verbal data and verbal commands; and

means for processing said one of received verbal data and received verbal command, said processed verbal commands being used to control one of a plurality of function and operations of said system, said processed speech data being one of said plurality of parameters for annotating said digital image.

11. The system of claim 1, further comprising means for determining said location of said system when said geographic location determining means is inoperable.

12. The system of claim 1, wherein said plurality of image data associated with said generation of said image includes one of an image mode, image quality, exposure duration, aperture length, light meter reading, flash status, lens focal length, auto focus distance, frame number, and a combination thereof.

13. In an image capturing system, a method for authenticating a captured image, comprising the steps of:

measuring a plurality of parameters associated with said captured image;

watermarking said plurality of parameters into said captured image to generate a watermarked image, and generating a verification key associated with said watermarked parameters;

extracting said plurality of parameters from said watermarked image with said associated verification key; and

comparing said extracted plurality of parameters from said watermarked image with said measured plurality of parameters associated with said captured image, whereby said captured image is authenticated if said extracted parameters match with said measured parameters.

14. The method of claim 13, further comprising the step of recording said measured plurality of parameters associated with each captured image, said extracted parameters being compared with said recorded parameters to authenticate said captured image.

15. The method of claim 14, further comprising the step of specifying which of said measured plurality of parameters is to be watermarked into a corresponding captured image.

16. The method of claim 14, further including the step of transmitting said watermarked image and said associated verification key to a remote system, and said extracting step and said comparing step are performed in said remote system.

17. The method of claim 14, further comprising the step of compressing said captured image prior to said watermarking step, whereby said measured parameters are watermarked into said compressed image.

18. A method for verifying the authenticity of a captured image, said captured image being generated by an image capturing system having means for measuring a plurality of parameters associated with said captured image and means for watermarking said plurality of parameters within said captured image, said method comprising the steps of:

specifying at least one of said plurality of parameters to be measured and watermarked by said image capturing system;

capturing an image of a desired object with said image capturing system;

watermarking said captured image of said object with said specified parameters;

generating a corresponding verification key based on said watermarked parameters;

storing said watermarked image and said corresponding verification key;

retrieving said watermarked image and said corresponding verification key;

extracting from said watermarked image said watermarked parameters using said verification key;

comparing said extracted parameters with said specified parameters to determine if said extracted parameters match said specified parameters.

19. The method of claim 18, further comprising the step of recording said specified parameters, wherein said recorded parameters are compared with said extracted parameters.

20. The method of claim 19, wherein said step of recording said specified parameters includes one of electronically recording said specified parameters with said captured image and manually recording said specified parameters associated with said captured image.

21. The method of claim 13, wherein the step of measuring a plurality of parameters associated with said captured image comprises receiving and recording object data from an object in an observed image frame when the image is generated, said object data comprising

object identification information.

22. The method of claim 18, wherein said plurality of parameters to be measured and watermarked comprises user data that is automatically transmitted from a user and recorded when said image is captured, said user data comprising user identification information.